Cyber Security in Cyber Space

James D. Lee Jr.
Old Dominion University

James D. Lee Jr

OLD DOMINION UNIV

Date: April 12, 2023

Cyber Security in Cyber Space

Introduction

For almost twenty years, the Internet has been a driving force in global communication and an integral part of people's everyday lives. As a result of technical developments and declining prices, over 3 billion people worldwide now utilize the Internet. The Internet has created a global infrastructure, and it is worth billions of dollars annually to the global economy (Judge et al.). Today's economic, commercial, cultural, social, and governmental activities and exchanges occur in Cyberspace, involving individuals, enterprises, non-profit organizations, and government and governmental agencies (Aghajani and Ghadimi 220). Cyberspace is the birthplace of much of the world's most essential and sensitive data, produced by transferring vital and sensitive information to it and developing fundamental and sensitive infrastructures and systems. (Akhavan-Hejazi and Mohsenian-Rad). Also, most citizens spend time and energy interacting in this arena, which has become the focal point of media migration and financial transactions (Siniosoglou et al.)

Most of a country's material and spiritual resources are invested in Cyberspace, and most of an individual's material and spiritual resources are either gained from or have a substantial influence on it (Amir and Givargis). That is to say, many facets of individuals' lives depend on this area, and its instability, insecurity, and difficulties have an impact beyond its borders (Li et al.). For example, figure 1 shows the projected cost of cybercrimes worldwide as the negative impact of insecure Cyberspace.

Nonetheless, governments face new security threats in the digital realm. Due to the low barrier to entrance, anonymity, the ambiguity of the unstable geographical region, the dramatic impact, and the lack of public transparency in Cyberspace, there are powerful and weak actors in Cyberspace, including governments, organized and terrorist organizations, and even individuals (Li and Qinghui). It distinguishes cyber risks from conventional national security concerns, which tend to be more obfuscated and whose actors can typically be traced back to certain governments and states in a specific region (Sarker). Analysts have speculated on the effects of cyber assaults for over a decade (Shin et al.). A virus's purpose may be described as an attack on the financial papers of an economic system or a disruption of a country's stock market. It is also possible for severe and potentially widespread physical or economic harm to arise from delivering an inaccurate message that causes a country's power plant to halt and fail or interrupt the air traffic control system, which adds to air mishaps (Li and Qinghui).

Cyberspace threats

When nations launch cyberattacks, they break into other countries' computer systems or networks to wreak havoc or disrupt normal operations (Motsch et al.). The sheer size of Cyberspace worldwide inevitably results in overlapping spheres of influence for nations with varying legal and cultural orientations and competing geopolitical goals (Li and Qinghui). Cyberspace has grown highly integrally to global communication and government. In turn, it is now difficult for any nation to function independently of it. Hence, Cyberspace significantly impacts the duties and responsibilities of each nation's security apparatus (Zhao et al.). Establishing assurances in the product supply chain process is impossible due to the worldwide nature of software and hardware creation. The cyber realm is qualitatively distinct due to its scalability. Cyberthreats can have far-reaching implications, but the system can control real-world activity since even the most giant bombs have a limited physical range. As in many other research areas, a small subset of the population is responsible for the most cyber activity. Users

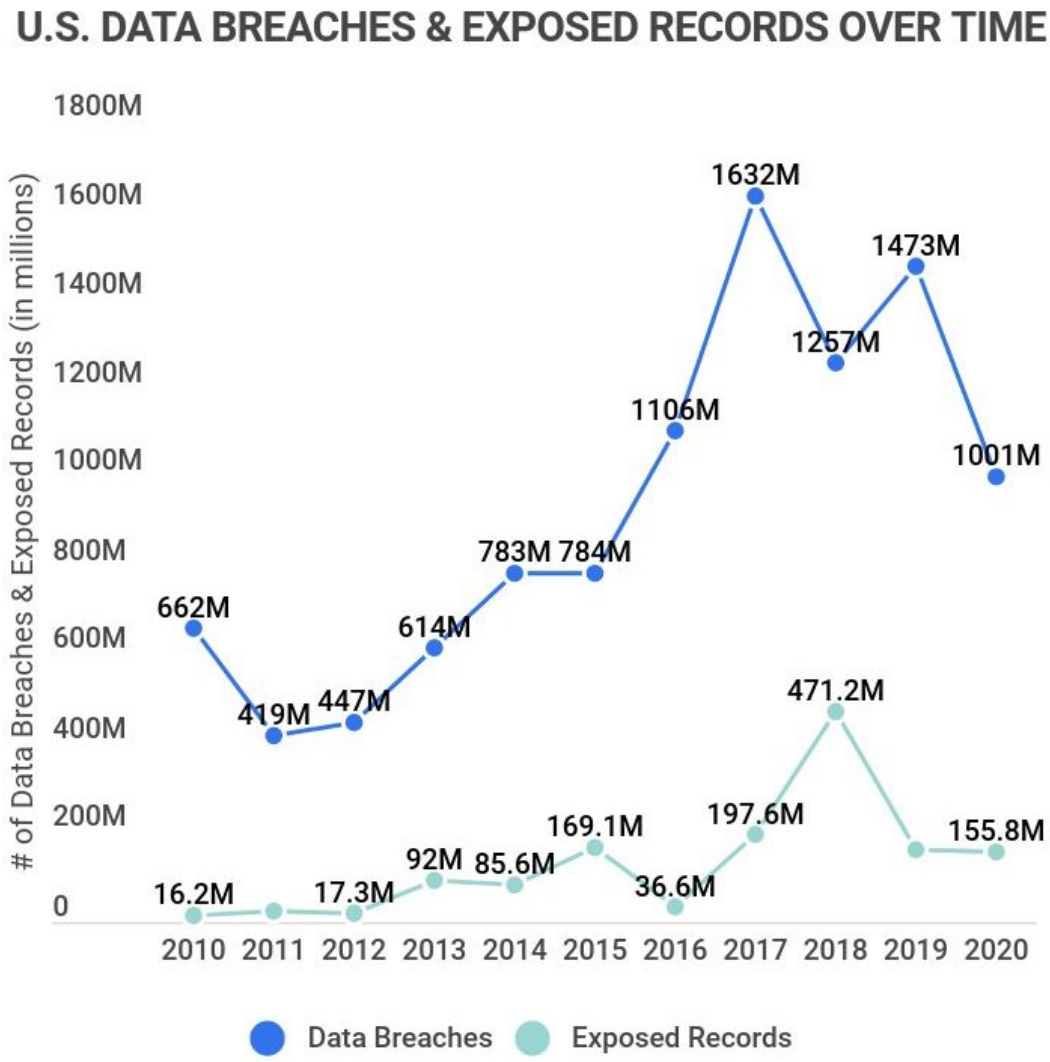
have no control over the system and cannot see how it works. It is well-known that only a few have the skills to effectively manage or coordinate cyber activities (Gholami and Erwin).

Despite the great degree of concentration and competence that would be required, the decentralized nature of the cyber domain makes it difficult for any individual or group of people to exercise complete control. The dynamic nature of information and communication technologies lies at the heart of Cyberspace's rapid development. Accordingly, cyber cohesion increases this rate of motion significantly. Each change ushers in a brand-new era of receptivity and responsiveness. Ultimately, Cyberspace is not a static place but rather an ever-changing one (Li and Qinghui).

Cyber assets can be found in various institutional settings with unique capabilities and resources (Zhao et al.). Ultimately, Cyberspace's anonymity makes it difficult, if not impossible, to pinpoint who is responsible for a particular conduct. Cyber threats may be broken down into four categories: those from outside, those from within, those posed by the supply chain, and those posed by local forces with insufficient operational competence (Al-Ghamdi). Some foreign governments use cyber technologies for espionage and intelligence gathering. Abuse and destruction of internet networks, embedded processors and controllers in critical sectors, and computer systems worldwide have been reported several times. There has been an increase in the number of attacks by criminal organizations that aim to steal money by breaching computer networks (Li and Qinghui). Fig 2 shows the data breaches and exposed documents over the years. Data breaches were highest in 2016, and more records were exposed in 2018.

Fig 2. U.S. Data Breaches and Exposed Records. Boskamp, Elsie. *Cybersecurity Statistics. 2023*. Web. April 12, 2023. < https://www.zippia.com/advice/cybersecurity-statistics/>

In addition, outsider hackers periodically get access to the network and make their opinions known. As things stand, even very inexperienced persons may easily penetrate networks by downloading the necessary software and protocols of the Internet and then using them against other sites. Web servers and email providers are among the targets of attacks by a separate organization (dubbed "Hackertivism") with political goals. These groups frequently



penetrate websites to propagate their political ideas, in addition to overwhelming email providers. (Solomon). However, disgruntled employees working within an organization are the most common perpetrators of cybercrime. They typically do not need extensive cyber-attack training because they already have insider access to the target system. Terrorists are another danger because they aim to compromise national security, inflict severe damage, devastate the economy, and erode public confidence by destroying, crippling, or deliberately exploiting critical infrastructure. (Saxena and Gayathri).

Denial of service assaults, logical bombs, abuse tools, sniffers, Trojan horses, viruses, worms, spam distribution networks, and botnets are common. In the denial of service technique, legitimate users and the system are denied access. In reality, the attacker begins

flooding the target systems with messages and immediately obstructs the legitimate data flow. As a result, no device can connect to the web or exchange data with other devices (Li and Qinghui).

Another tactic is termed distributed denial of service attacks, and instead of coming from a central location, they come from many different systems all at once. It is commonly accomplished by spreading worms throughout a network of computers. Users of varying skill levels can gain access to abuse tools that can locate and exploit vulnerabilities in a network. The "logic bomb" is another attack of harmful code introduced into a program if a specific condition is satisfied (Li, Sun, and Qingyu). By analyzing each data packet, sniffer programs may steal critical information like passwords from a network. Trojan horses are harmful applications that masquerade as necessary downloads or updates. Viruses were also corrupt otherwise usable programs (called "system files") by placing copies of themselves there. These variants spread the virus by loading infected files into memory and running them. Viruses, in contrast to worms, cannot replicate without help from humans. In contrast, the worm is a self-replicating program that spreads from computer to computer inside a network (Li and Qinghui).

Last but not least, a Botnet is a collection of compromised computers that work together to launch coordinated assaults, spam other users, and steal their personal information. Botnets are typically placed covertly on the victim's computer, granting the hacker remote access and control over the compromised machine. Electronic warriors is another name for botnets. (Kharlamova, Seyedmostafa, and Chresten).

Cybersecurity

Organizations of all sizes and types need to take steps to ensure the safety of their IT infrastructure from cyberattacks. The success of a cybersecurity company hinges on its ability to keep private data and customer records out of the hands of its competitors. Clients and

consumers are the targets of abuse from businesses and their rivals. For a company or organization to thrive, it must first create a reputation for providing this safety (Rodrguez-deArriba et al.). Cybersecurity involves taking real-world steps to prevent unauthorized access to computer systems, networks, and data. Professionals in cybersecurity keep the Internet, private networks, and other computer systems safe. Cybersecurity restricts access to sensitive data to those who need it. Knowledge of the many forms of cybersecurity is essential for optimal safety (Li and Qinghui).

Network security aims to keep harmful programs and unauthorized users out of a network. Network security describes firms' precautions to protect their computer networks from threats like viruses and hackers (Pokhrel and Tsokos). In contrast, application security refers to using technological safeguards—including anti-virus software, encryption, and firewalls to prevent unauthorized access to and manipulation of software programs (Li and Qinghui).

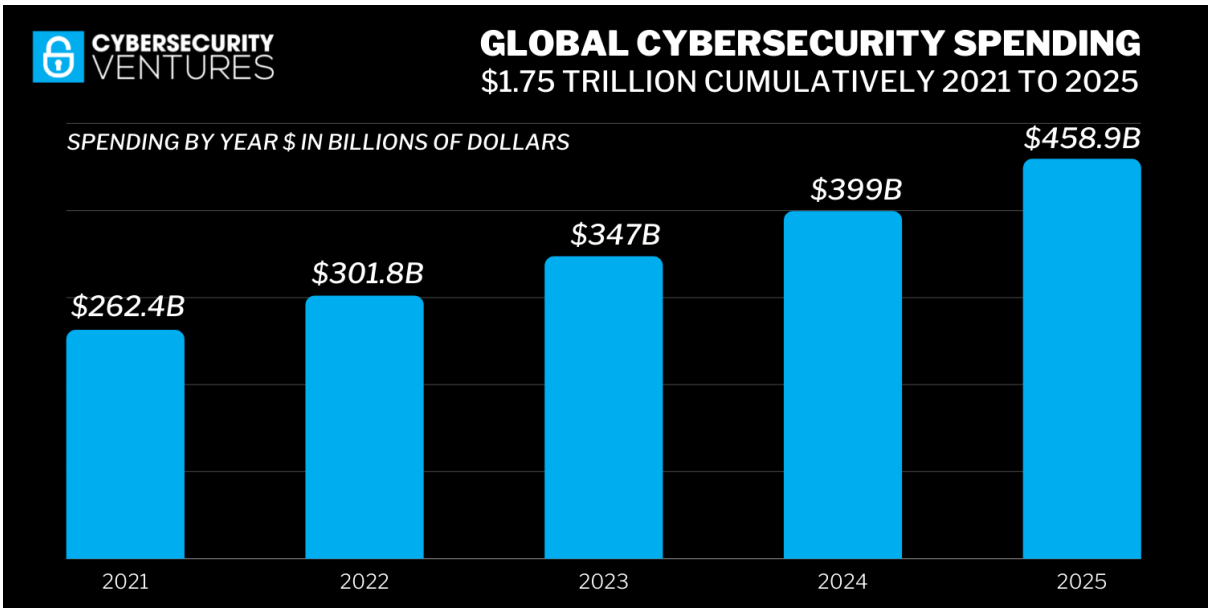
Further, information security safeguards records and files against threats like loss, theft, tampering, and deletion. Data control and protection procedures are part of operational security. For instance, processes that dictate when and where data may be kept or exchanged and user rights for network access. Besides, safeguarding data stored in the cloud (through associated software) and monitoring things to prevent local assaults is linked to cloud security (Li and Qinghui). Accordingly, companies all over the world spend extensive financial resources on cybersecurity. Fig 3 identifies global cybersecurity spending from 2021 to 2025. In 2021, the expenditure was $262B, expected to be $458.9B by 2025.

Fig 3. Spending on Cybersecurity. Braue, David. *Global Cybersecurity Spending To Exceed $1.75 Trillion From 2021-2025.* 2021. Web. April 12.

2023. < https://cybersecurityventures.com/cybersecurity-spending-2021-2025/>

Cyber Security Measures

Practicing good cyber hygiene is essential for keeping digital assets safe from intrusion. The proliferation of cyber threats is a stark reality in today's online environment. Everyone,



from a person to large corporations, must practice good cyber hygiene to protect themselves against hacking, viruses, and other online dangers. Individuals and groups of organizations must adopt specific policies and practices to identify the most vulnerable points of connection and security backdoors. Addressing security concerns from every angle, including application development, infrastructure reinforcement, arrangement testing, Bring Your Device (BYOD) techniques, and employee awareness, is crucial. i.e., identifying and differentiating all internet-connected devices. Every connected device is at risk of constant digital threats and is vulnerable to cyberattacks. For cybercriminals, this creates a new entryway and point of attack (Singh et al.).

Moreover, devices and software should be prioritized and graded according to how sensitive they are and how much data they expose. The workload of system administrators and

security engineers is lightened as a result. Devices, frameworks, and applications should be hardened to make them more secure and reduce the entry point for a cyber attack. Information encryption, audits of safe settings, password restrictions, and two-factor authentication are all rolled into one convenient package. Further, security patches implement patch and vulnerability management across all devices and systems. According to research on data breaches conducted by Verizon in 2015, many previously exploitable flaws persist because previously available security patches were never implemented. Several flaws are traced back to 2007 (Singh et al.).

In addition, businesses should have a reliable backup plan in place. Regularly reinforcing crucial information is a component of a reinforcement strategy for data protection, and it is the final line of defense against data loss or theft. The only way to ensure retrieving genuine data from reinforcement is to incorporate a data recuperation technique (Rajasekharaiah, Dule, and Sudarshan). Last but not least, training in cyber hygiene practices that is both effective and cost-efficient is essential. Information security relies on many layers of protection, the first of which is education, as stated by the European Network and Information Security Agency. Practical training starts with a person and includes educating customers and employees, creating a customer education program to help them learn to recognize potential security concerns, and so on (Singh et al.).

Also, it is generally agreed that the current state of security modeling calls for reflection due to its piecemeal and regional focus. Cybersecurity maturity models have taken the field in an interesting new direction. Managers can improve their company's cyber security using maturity models. They provide improved security risk management, lead to monetary savings, encourage introspective growth, and underpin solid protection practices and procedures. Instead of activating security measures without thinking about the organization, they push everyone toward security maturity, as shown by the model. Despite these advantages, maturity

models only give a basic compliance model rather than an ideal cyber security model that can adapt to the ever-changing nature of the cyber landscape and the increasing complexity of the threats within it (Le and Hoang).

In today's complex online world, businesses of all types and sizes need to take extra precautions to protect their customers' private data. When it comes to cyber security and individual cyber assaults, social media plays a significant role. Since most employees now use social media or networking sites almost daily, this opens up a huge opportunity for cybercriminals to get unauthorized access to sensitive data and steal valuable intellectual property. These days, it is simple to spread sensitive data, so companies need to be prepared to spot and rapidly address any data breaches that may occur. Hackers may gain access to sensitive information from social media users. Consequently, users must take appropriate precautions to protect themselves against the possible abuse and loss of data they provide on these platforms (Reddy, Nikhita, and Reddy).

Conclusion

The effects of cyber threats on national and economic security are substantial. It is widespread, violent, all over the place, and getting more complex daily. Having a cyber security function in all components is essential for future growth, innovation, and competitive advantage since there are substantial concerns for various industry agencies and public and private organizations for enterprises and governments alike. Companies can adopt multiple solutions, such as cyber hygiene, authentication, firewall, malware scanners, etc. However, training and development of stakeholders are needed to protect intellectual property. Besides, cyber threats develop with new technologies and trends. Hence, companies must focus on

continuously updating cyber security systems, including a network and applications, among others, focusing on new software.

We have discussed some positive uses of Cyberspace. The boundaries between what is real and what is virtual are decreasing as technology improves. Cyberspace may dehumanize us, leading to a crisis of identity. Computers offer clinical precision during warfare that alienates us from realities. The Internet is growing in popularity and slowly becoming part of our lives. Cyberspace is invasive. So we need to understand the technology and identify when it is used and when it is being abused. When we understand these things, Cyberspace becomes a valuable tool.

Resource Page

Aghajani, Gholamreza, and Noradin Ghadimi. "Multi-objective energy management in a micro-grid." *Energy Reports* 4 (2018): 218-225.

Akhavan-Hejazi, Hossein, and Hamed Mohsenian-Rad. "Power systems big data analytics: An assessment of paradigm shift barriers and prospects." *Energy Reports* 4 (2018): 91-100.

Al-Ghamdi, Mohammed I. "Effects of knowledge of cyber security on prevention of attacks." *Journal of Basic and Applied Sciences* 10 2021:1-3.

Amir, Maral, and Tony Givargis. "Pareto optimal design space exploration of cyber-physical systems." *Internet of Things* 12 (2020): 100308.

Boskamp, Elsie. *Cybersecurity Statistics.* 2023. Web. Apr 12, 2023. < https://www.zippia.com/advice/cybersecurity-statistics/>

Braue, David. *Global Cybersecurity Spending To Exceed $1.75 Trillion From 2021-2025.* 2021. Web. April 12. 2023. < https://cybersecurityventures.com/cybersecurity-spending-2021-2025/>

Fleck, Anna. *Cybercrime Skyrocketing in the Following Years. 2022.* Web. April 12. 2022. < https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/>

Gholami, Ali, and Erwin Laure. "Security and privacy of sensitive data in cloud computing: a survey of recent developments." *arXiv preprint arXiv:1601.01498* 2016.

Judge, Malik Ali, et al. "Price-based demand response for household load management with interval uncertainty." *Energy Reports* 7 2021: 8493–8504.

Kharlamova, Nina, Seyedmostafa Hashemi, and Chresten Træholt. "Data-driven approaches for the cyber defense of battery energy storage systems." *Energy and AI* 5 (2021): 100095.

Li, Jian, Chaowei Sun, and Qingyu Su. "Analysis of cascading failures of power cyber-physical systems considering false data injection attacks." *Global Energy Interconnection* 4.2 2021: 204–213.

Li, Nianyu, et al. "Early validation cyber–physical space systems via multi-concerns integration." *Journal of Systems and Software* 170 2020: 110742.

Li, Yuchong, and Qinghui Liu. "A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments." *Energy Reports* 7 (2021): 8176-8186.

Motsch, William, et al. "Approach for dynamic price-based demand side management in cyber-physical production systems." *Procedia Manufacturing* 51 2020: 1748-1754.

Pokhrel, Nawa Raj, and Chris P. Tsokos. "Cybersecurity: a stochastic predictive model to determine overall network security risk using Markovian process." *Journal of Information Security* 8.2 (2017): 91-105.

Rajasekharaiah, K. M., Chhaya S. Dule, and E. Sudarshan. "Cyber security challenges and its emerging trends on latest technologies." *IOP Conference Series: Materials Science and Engineering*. Vol. 981. No. 2. IOP Publishing, 2020.

Reddy, G. Nikhita, and G. J. Reddy. "A study of cyber security challenges and its emerging trends on latest technologies." *arXiv preprint arXiv:1402.1842* 2014.

Rodríguez-deArriba, María-Luisa, et al. "Dimensions and measures of cyber dating violence in adolescents: A systematic review." *Aggression and Violent Behavior* 58 (2021): 101613.

Sarker, Iqbal H. "CyberLearning: Effectiveness analysis of machine learning security modeling to detect cyber-anomalies and multi-attacks." *Internet of Things* 14 2021: 100393.

Shin, Jinsoo, et al. "Application of STPA-SafeSec for a cyber-attack impact analysis of NPPs with a condensate water system test-bed." *Nuclear Engineering and Technology* 53.10 2021: 3319–3326.

Singh, Debabrata, et al. "Cyber-hygiene: The key concept for cyber security in cyberspace." *Test Engineering and Management* 83 2020: 8145–8152.

Siniosoglou, Ilias, et al. "A unified deep learning anomaly detection and classification approach for smart grid environments." *IEEE Transactions on Network and Service Management* 18.2 2021: 1137–1151.

Solomon, Rukundo. "Electronic protests: Hacktivism as a form of protest in Uganda." *Computer Law & security review* 33.5 2017: 718–728.

Varga, Stefan, Joel Brynielsson, and Ulrik Franke. "Cyber-threat perception and risk management in the Swedish financial sector." *Computers & Security* 105 (2021): 102239.

Zhao, Jun, et al. "TIMiner: Automatically extracting and analyzing categorized cyber threat intelligence from social data." *Computers & Security* 95 2020: 101867

Zhao, Zi-gang, et al. "Control-theory based security control of cyber-physical power system under multiple cyber-attacks within the unified model framework." *Cognitive Robotics* 1 2021: 41–57.